LESSON 1: DIGITAL SIGNATURE – EDUCATING THE TRAVELER

LESSON TITLE	**DIGITAL SIGNATURE-EDUCATING THE TRAVELER**
SUMMARY	This lesson will provide an overview of digital signature, how it is used in the Defense Travel System and how to obtain your digital signature. It should be used in conjunction with viewing the PKI video.
DURATION	.50 Hours
TOPICS	**TOPIC TITLE** **DIGITAL SIGNATURE**
OBJECTIVES	At the end of this lesson, participants will be able to understand and explain: ▪ Digital Signature features ▪ Components of Digital Signature ▪ How to register for your digital signature ▪ Use of Digital Signature with DTS ▪ Where to go for help
MATERIALS	Instructor Guide, Briefing Materials, Participant Handout(s), PKI Video

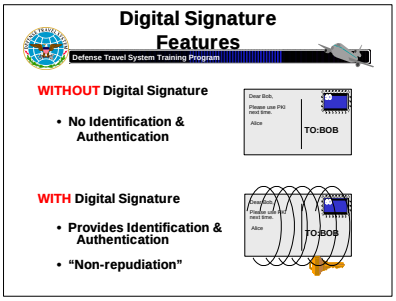
LESSON 1: DIGITAL SIGNATURE – EDUCATING THE TRAVELER

Slide 2

LESSON PLAN

At the end of this lesson, participants will be able to understand and explain:

(DISCUSS/EXPLAIN SLIDE)



Slide 3

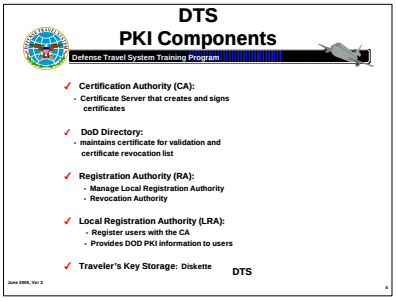
DIGITAL SIGNATURE FEATURES

When a digital signature is invoked, the following features are provided:

(1) **Identification & Authentication**: The receiver is assured that the sender is who they claim to be.
(2) **Data Integrity**: The sender and receiver are assured that the data has not been changed in any way.

A message sent on the Internet today is similar to sending a postcard to someone written in pencil. It can be read by anyone and the words easily changed. Using a digital signature on a message is similar to writing the words in ink and signing your name. Anyone can still read the words, however they cannot be easily changed without detection.

It should also be noted that a digitally signed document would be considered valid because it cannot be disavowed by the person who has digitally signed it – hence the legal term "non-repudiation".



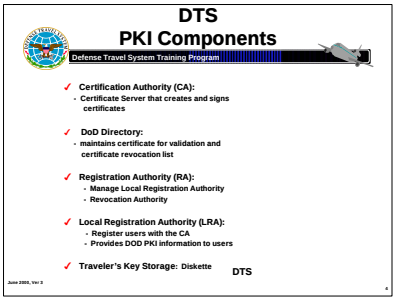
Slide 4

DTS PKI COMPONENTS

There are several PKI Components associated with digital signature and DTS. They are:

The Certification Authority (CA): The CA manages user registration and certificate generation, revocation, renewal, and archival. The CA is transparent to the users.

LESSON 1: DIGITAL SIGNATURE – EDUCATING THE TRAVELER



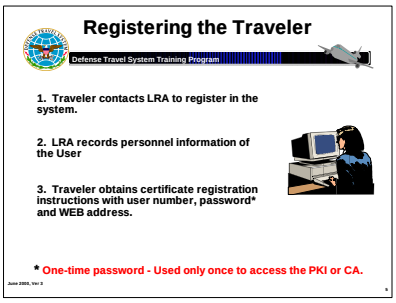
Slide 4 (Con't)

DoD Directory is where cerficates are maintained for validation and where the certificate revocatoin list is maintained.

The Registration Authority (RA) is responsible for registering and managing Local Registration Authorities (LRAs). The RA will manage LRA groups and LRA certificates. They are also responsible for revoking certificates should that become necessary.

The Local Registration Authority (LRA) is responsible for registering users by providing them with a unique user number and password. The LRA also provides the user's registration information to the CA.

Users will store their key on a 3.5" diskette. The diskette should be treated just as you would an ATM or credit card. While no classified information is contained on the diskette, it should still be safeguarded to ensure an unauthorized source couldn't use it. It's also a good idea to consider "write protecting" the diskette as an additional safeguard.

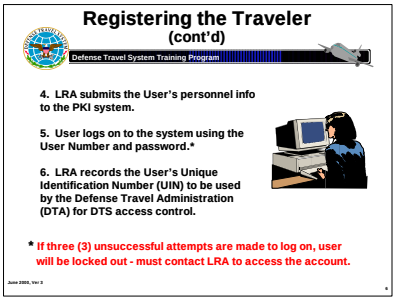


Slide 5

REGISTERING THE TRAVELER

The next two slides (5 & 6) explain the steps involved in registering a traveler so they can obtain a digital signature.

(DISCUSS/EXPLAIN EACH SLIDE)



Slide 6

NOTE FOR SLIDE 6

BE SURE TO EMPHASIZE THE IMPORTANCE OF THE LRA RECORDING THE USER'S UIN SO THAT IT MAY BE PASSED ON TO THE DTA. IF NOT RECORDED PROPERLY, THE USERS WILL BE UNABLE TO ACCESS THE DTS SYSTEM WITH THEIR DIGITAL SIGNATURE.

LESSON 1: DIGITAL SIGNATURE – EDUCATING THE TRAVELER

FOR TRAINING ONLY

DoD Public Key Infrastructure (PKI)
Certificate Registration Instructions

Require Photo ID before hand Delivery to:
Joe Test
Time Sensitive Material
Certificate Registration Instructions

Please read this sheet very carefully, and follow the instructions on it. Please DO NOT allow anyone to see the password on this page until you have completed the process described below! This page will help you to obtain your personal digital certificate. Others will use this certificate to electronically identify you. If you have any problems or questions, please notify your "Local Registration Authority," who is:

Jamil J. Nimeh
619-522-5403
DSN: 619-522-5112
jamil.j.nimeh@cpmx.saic.com

You Must register within thirty days. Please have a floppy disk ready. You will need it to store your digital certificate. With a web browser, type in the "Remite" or "Open Page" space

ds-2.den.disa.mil

and follow the instructions on that web site. (Please note that, at present, you must use the US version of Netscape Navigator or Communicator 4.05 or later. In the future, other brands will also be supported.)

You will be asked to compare a "Certificate Fingerprint". Ensure it is: 52:AG: D3:C9: 1/0:84: FE:CF:A4:AD:AE:69:33:36:95:6D

When asked by the web site to select a Certificate Authority, select CA-1. Later, you will be asked to fill in your User Number and Password. This password will only be used once, so you do not need to remember it.

Your User Number: 0008800188
Your Password: YAdACfaD

This is government information for official use only. Access to this information requires compliance to DoD standards and regulations. Criminal statues and regulations provide penalties for unauthorized access or use of this information.

FOR TRAINING ONLY

Slide 7

NOTE: Slide is very difficult to read so each participant should be provided with a "hard" copy of the information on this slide.

CERTIFICATE REGISTRATION INSTRUCTIONS

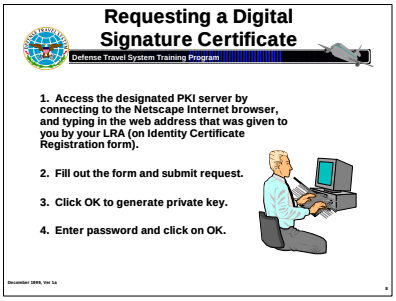
After the LRA sends the user's data to the CA, this form will print out on the LRA's dedicated, non-networked printer. This form is the Certificate Registration Instructions page; it has the User Number, password and the WEB address the user should contact to request the certificate and generate their public/private key pair. This information should be protected by the user because anyone could use this information to log on as the user and generate the keys under a false name - your name - and assume your identity.

The form has a lot of important user information, so the LRA should make sure they read and understand. There is also special information at the bottom of the form that helps the user with the password.

After the user receives their Certificate Registration Instructions page from their LRA, they are ready to go to a terminal to generate their certificate. It's really a very simple process – just follow the instructions displayed on each screen. When in doubt, contact your LRA for assistance.

NOTE - Users should be reminded to carefully read the instructions on each screen. If the users would like, they can print out the instructions on the screen or just move the windows in front of the screen to read the instructions on the original screen.

LESSON 1: DIGITAL SIGNATURE – EDUCATING THE TRAVELER



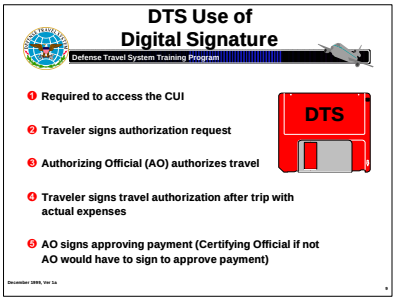
Slide 8

REQUESTING A DIGITAL SIGNATURE CERTIFICATE

This slide depicts the steps that should be followed when requesting a digital signature certificate.

(DISCUSS/EXPLAIN SLIDE)

The LRA uploads user data files and also unlocks the user terminals. When a user logs on to the system to generate their keys, they will use the user number and password received from the LRA. Remember, as we saw learned on the previous slides, if the user makes three (3) unsuccessful attempts to access the system, the user will be locked out and will be required to call their LRA to unlock the account.



Slide 9

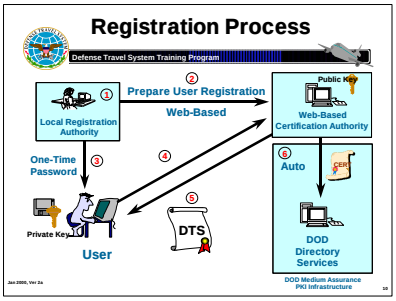
DTS USE OF DIGITAL SIGNATURE

This slide briefly explains when to use your 3.5' diskette during the trip process using the Defense Travel System.

(DISCUSS/EXPLAIN SLIDE)

(Mention that it is envisioned that the 3.5" diskette will most likely be changed to some type of "smart card" in the future.)

LESSON 1: DIGITAL SIGNATURE – EDUCATING THE TRAVELER



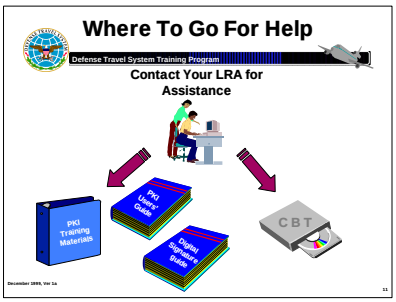
Slide 10

Note: This slide begins to "build" with each mouse click. Follow the numbers with the corresponding script information.

REGISTRATION PROCESS

Now that we have discussed all the components and steps, let's review this chart and walk through the entire registration process from start to finish: **(follow the numbers on the slide)**

1. The LRA inputs the User's personal information into the system.
2. The LRA than uploads information about the user to the PKI CA, a special server located at a Defense Megacenter (DMC). The information given to the server includes a user number and a password for the authorized user.
3. The LRA verifies the user's identity and provides them with their user number and password.
4. The User connects to the CA using their WEB browser. The key pair is automatically generated in the browser, and the private key stored to their hard drive. The user will than save the private key to a floppy diskette and delete the file from the hard drive. The user's public key is automatically sent to the CA with the request to issue a certificate. After the CA verifies the user number and password, it generates the certificate.
5. The CA passes a copy of the certificate back to the user, and
6. Automatically posts a copy of the certificate in the directory server to make the public key available to others.



Slide 11

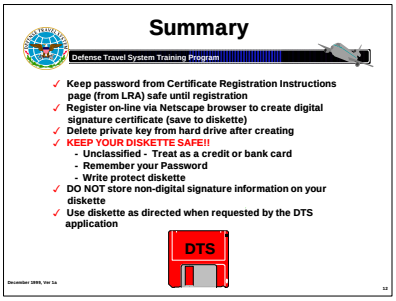
WHERE TO GO FOR HELP

When you have questions or problems on digital signature or when requesting your certificate and public/private key pair, the first place you should go is your LRA.

For steps on how to obtain a user certificate, your LRA will be provided with references like the computer-based training (CBT) modules to help you. The LRA will also have step-by-step user guides.

For technical issues, your LRA may not have the answer right away, but will know whom to contact.

LESSON 1: DIGITAL SIGNATURE – EDUCATING THE TRAVELER



Slide 12

Digital Signature Security

Let's take a minute to summarize some of the things that the user needs to remember after they have obtained their digital signature.

(Review/Discuss Slide)

Slide 13

This concludes the lesson on digital signature and how a user will obtain their registration certificate. Detailed instructions for the user on obtaining their certificate and signature will be found on the screen shots when logged on to the web and also on the screen shots included in the user guide that is provided on the training CD.

QUESTIONS?